SPECIFICATION

TITLE

AUTHENTICATION SYSTEM, AUTHENTICATION METHOD, AUTHENTICATION APPARATUS, AND AUTHENTICATION METHOD THEREFOR

BACKGROUND OF THE INVENTION

Field of the Invention

The present invention relates to authentication systems, authentication methods, authentication apparatuses, and authentication methods therefor, and more particularly, to an authentication apparatus which efficiently uses advantages of different types of encryption methods to perform encryption.

Description of the Prior Art

As authentication and signature methods in authentication systems, there have been conventionally used a common-key encryption method and a public-key encryption method.

In the common-key encryption method, one encryption key called a common key is used and information encrypted by the common key is decrypted by the same common key. Since the common-key encryption method performs encryption and decryption within a short period, it is used in cases where information which requires high-speed processing is processed, such as electronic money or commuter-pass information stored in an IC card.

In the public-key encryption method, two encryption keys called a public key and a private key are used, and information encrypted by one encryption key is decrypted by the other encryption key. The public-key encryption method has a higher safety in terms of information leakage but has a lower processing speed than the common-key encryption method, and is used in cases where anonymity is required, such as a case in which a financial transaction is achieved on a network, such as the Internet.

When the public-key encryption method is used, an IC card stores a certificate for certifying the user who uses the IC card and a public key, and is used as an encryption module.

Depending on fields to which authentication systems are applied, the common-key encryption method or the public-key encryption method is used.

It has been demanded these days, however, that an encryption method be created which has both safety provided by the public-key encryption method and quickness provided by the common-key encryption method, in order to allow one IC card to enable efficient authentication and a financial transaction.

Authentication systems have the ability to check the legitimacy of a certificate stored in an IC card, but do not have the ability to check whether the IC card is actually used legitimately.

In authentication systems, if an IC card is lost, since procedures for authentication and a financial transaction by the use of the IC card is stopped according to a certificate invalidation list periodically issued from a certification authority provided on a network, the use of the IC card performed real time at any points on the network cannot be stopped immediately.

SUMMARY OF THE INVENTION

The present invention has been made in consideration of the foregoing points. It is an object of the present invention to provide an authentication system, an authentication method, an authentication apparatus, and an authentication method therefor which has improved safety and quickness for authentication.

The foregoing object is achieved in one embodiment of the present invention through the provision of a user authentication system including a data holding medium for holding the common key unique to a user, used in the common-key encryption method; an authentication apparatus for holding the common key used in the common-key encryption method and the private key used in the public-key encryption method, each unique to the user; and an information processing apparatus connected to the authentication apparatus in an always-communicable manner and provided with a function for performing authentication by the public-key encryption method; wherein the authentication apparatus performs authentication by using the common key held by the data holding medium and the common key held by the authentication apparatus, in response to a user authentication request sent from the information processing apparatus, and only when the user has been authenticated, performs processing for making the information processing apparatus authenticate

the user by using the private key corresponding to the user. As a result, according to this authentication system, user authentication is performed with safety provided by the public-key encryption method and quickness provided by the common-key encryption method.

The foregoing object is achieved in another aspect of the present invention through the provision of a user authentication method for a user who carries a data holding apparatus for holding a common key used in the common-key encryption method, including a step of authenticating the user by the common-key encryption method by using the common key held by the data holding apparatus of the user in response to a user authentication request; and a step of, only when the user has been authenticated, performing processing for authenticating the user by the public-key encryption method. As a result, according to this authentication method, user authentication is performed with safety provided by the public-key encryption method and quickness provided by the common-key encryption method.

The foregoing object is achieved in still another aspect of the present invention through the provision of an authentication method including a step of holding a common key used in the common-key encryption method and a private key used in the public-key encryption method, for each user; an authentication step of, in response to a user authentication request sent from an external information processing apparatus, authenticating the user by using the held common key for the user and a common key used in the common-key encryption method which the user has and is held by a data holding apparatus; and a step of, only when the user has been authenticated in the authentication step, performing processing for making the information processing apparatus authenticate the user by the public-key encryption method by using the private key corresponding to the user. As a result, according to this authentication method, user authentication is performed with safety provided by the public-key encryption method and quickness provided by the common-key encryption method.

The foregoing object is achieved in yet another aspect of the present invention through the provision of an authentication apparatus including a holder for holding a common key used in the common-key encryption method and a public key used in the public-key encryption method, for each user; and an authenticating device

which, in response to a user authentication request sent from an external information processing apparatus, authenticates the user by using the common key for the user held by the holder and a common key used in the common-key encryption method for the user held by a data holding medium of the user, and for, only when the user has been authenticated, performing processing for making the information processing apparatus authenticate the user by the public-key encryption method by using the private key corresponding to the user. As a result, according to this authentication apparatus, user authentication is performed with safety provided by the public-key encryption method and quickness provided by the common-key encryption method.

As described above, according to the present invention, an information holding medium stores the common key of the user used in the common-key encryption method, and, in response to a user authentication request sent from an information processing apparatus, the user is authenticated by the common-key encryption method by using the common key stored in the information holding medium of the user. Only when the user has been authenticated, predetermined processing for making the information processing apparatus authenticate the user by the public-key encryption method is performed. Therefore, user authentication provided with quickness given by the common-key encryption method and safety given by the public-key encryption method is performed. Thus, an authentication system, an authentication method, an authentication apparatus, and a method therefor which have improved safety and quickness for authentication are provided.

Additional features and advantages of the present invention are described in, and will be apparent from, the Detailed Description of the Preferred Embodiments and the Drawings

DESCRIPTION OF THE DRAWINGS

Fig. 1 is an outlined view showing the structure of a network system according to an embodiment of the present invention;

Fig. 2 is a block diagram showing the structure of a user terminal;

Fig. 3 is a block diagram showing the structure of an IC card;

Fig. 4 is a block diagram showing the structure of a WWW server;

Fig. 5 is a block diagram showing the structure of a security server;

Fig. 6 is an outlined view showing authentication;

Fig. 7 is a flowchart of an authentication procedure achieved by the user terminal;

Fig. 8 is a flowchart of an authentication procedure achieved by the security server;

Fig. 9 is an outlined view showing the structure of a common-key data base;

Fig. 10 is an outlined view showing the structure of a user-certificate data base;

Fig. 11 is an outlined view showing the structure of a certificate;

Fig. 12 is an outlined view showing writing;

Fig. 13 is a flowchart of a writing procedure achieved by the user terminal; and

Fig. 14 is a flowchart of a writing procedure achieved by the security server.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

An embodiment of the present invention will be described below in detail by referring to the drawings.

(1) Structure of a network system according to an embodiment

Fig. 1 shows a network system 1 according to an embodiment of the present invention as a whole. The network system 1 is formed of a world-wide-web (WWW) server 3 installed in a service provider 2, a user terminal 4, and a security server 6 installed in an authentication center 5 all of which are connected via the Internet 7.

The user terminal 4 is a general personal computer, as shown in Fig. 2, in which a central processing unit (CPU) 10, a read only memory (ROM) 11 storing programs for executing various types of processing, such as that described later, a random access memory (RAM) 12 serving as a work memory for the CPU 10, and an input and output section 14 serving as an input and output interface are connected via a bus 13, and a network interface 15 formed of a modem, an IC-card reading and writing unit 9, a console 17 formed of a keyboard, a monitor, a mouse, and the like, and a storage unit 18 formed of a hard disk unit are connected to the input and output section 14.

The storage unit 18 stores a WWW browser program 19, an encryption library 25 formed of programs which manage encryption according to the common-key encryption method and the public-key encryption method, and an IC-card driver 21 for the IC-card reading and writing unit 9.

When the CPU 10 develops the WWW browser program 19 stored in the storage unit 18, on the RAM 12 and executes it, the CPU 10 functions as a WWW browser 22 (Fig. 1) and is allowed to send and receive information on the Internet 7 through the network interface 15.

When the CPU 10 develops a program of the encryption library 20 stored in the storage unit 18, on the RAM 12 and executes it, the CPU 10 functions as an encryption module 23 (Fig. 1) to manage encryption.

Between the WWW browser 22 and the encryption module 23, an application program interface (API), such as that conforming to a public-key cryptography standard #11 (PKCS #11)-24 standard provided by RSA, is provided to make information exchange easy between the WWW browser 22 and the encryption module 23.

In addition, the CPU 10 develops the IC-card driver 21 on the RAM 12 and executes it to operate the IC-card reading and writing unit 9.

The IC-card reading and writing unit 9 is provided with a radio function conforming, for example, to a Bluetooth standard to send information read from an IC card 8 by radio to the storage unit 18 and to write information received from the storage unit 18 into the IC card 8 by radio.

The IC card 8 is formed, as shown in Fig. 3, of a CPU 27, a ROM 28, a RAM 29, a radio-communication interface 30 for radio communication with the IC-card reading and writing unit 9, and an electrically erasable programmable ROM (EEPROM) 31 which stores various types of information, such as a user ID assigned to the IC card 8, all of which are connected via a bus 26.

The EEPROM 31 has a user-ID area 32, an electronic-priced-information area 33, and a common-key area 34. A user ID, electronic priced information, and a common key for allowing an external access to be made to the user-ID area 32 and the electronic-priced-information area 33 are written into the corresponding areas.

The CPU 27 develops an encryption processing program stored in the ROM 28, on the RAM 29 and executes it to decrypt information (hereinafter called common-key-encrypted information) encrypted by a common key obtained through the radio interface 30, by using the common key read from the EEPROM 31.

When the common-key-encrypted information is successfully decrypted by using the common key read from the EEPROM 31, the CPU 27 permits access to each area of the EEPROM 31, and, for example, writes electronic priced information obtained through the radio interface 30 into the electronic-priced-information area 33 of the EEPROM 31.

The WWW server 3 installed in the service provider 2 is formed, as shown in Fig. 4, of a CPU 36, a ROM 37, a RAM 38, and an input and output section 40, all of which are connected via a bus 39, and a network interface 41 formed of a router for connecting the input and output section 40 to the Internet 7, a management console 42 formed of a keyboard, a monitor, a mouse, and the like, and a storage unit 43, all of which are connected. The storage unit 43 stores a WWW server program 44 and service contents 45, such as electronic priced information.

When the CPU 36 develops the WWW server program 44 stored in the storage unit 43 on the RAM 38 and executes it, the CPU 36 functions as the WWW server 3 (Fig. 1) and is allowed to offer the service contents 45 through the network interface 41.

In contrast, the security server 6 installed in the authentication center 5 is formed, as shown in Fig. 5, of a CPU 46, a ROM 47, a RAM 48, and an input and output section 50, all of which are connected via a bus 49, and a network interface 51 formed of a router for connecting the input and output section 50 to the Internet 7, a management console 52 formed of a keyboard, a monitor, a mouse, and the like, and a storage unit 53, all of which are connected. The storage unit 53 stores a security server program 54, a user-certificate data base 55, described later, and a common-key data base 56, described later.

When the CPU 46 of the security server 6 develops the security server program 54 stored in the storage unit 53 on the RAM 48 and executes it, the CPU 46 functions as the security server 6.

(2) Authentication procedures

In the network system 1, as shown in Fig. 6, the user terminal 4 performs authentication according to an authentication procedure RT1 for authenticating itself shown in Fig. 7 and the security server 6 authenticates the user terminal 4 according to an authentication procedure RT2 shown in Fig. 8, so that the user terminal 4 proves the legitimacy of itself to the WWW server 3, which provides electronic priced information.

In this case, the user terminal 4 first operates the WWW browser 22 to request the WWW server 3 to send electronic priced information to the user terminal 4.

The WWW server 3 generates trial characters formed of a random character string, and then sends an authentication request command C1 for authenticating the user terminal 4 in order to check the legitimacy of the information request source, together with the generated trial characters to the user terminal 4.

When the CPU 10 of the user terminal 4 receives the authentication request command C1, the CPU 10 starts the authentication procedure RT1 (in step SP1), and sends the received authentication request command C1 and the trial characters to the encryption module 23 (in step S2).

Then, the CPU 10 reads a user ID from the IC card 8 through the IC-card reading and writing unit 9, and sends the authentication request command C1 and the trial characters received by the encryption module 23, to the security server 6 together with the read user ID (in step S3).

When the CPU 46 of the security server 6 receives the authentication request command C1, the CPU 46 starts the authentication procedure RT2 (in step SP11), reads the common key corresponding to the received user ID from the common-key data base 56 shown in Fig. 9, stored in the storage unit 53 (in step SP12), and generates common-key encrypted information by the use of the read common key. Then, the CPU 46 sends an IC-card authentication request command C2 together with the common-key-encrypted information to the encryption module 23 of the user terminal 4 (in step SP23).

The CPU 46 reads the certificate 58 corresponding to the user ID from the user-certificate data base 55 shown in Fig. 10, stored in the storage unit 53, and sends

it in advance to the encryption module 23 of the user terminal 4 and to the WWW server 3 through the WWW browser 22.

In the certificate 58, if it is, for example, for a user ID 0001, information is written such as a certificate serial number, expiration-date information of the certificate, the user ID, a public key generated as a pair with the private key, an electronic-mail address, and the contact information of the user, as shown in Fig. 11. In addition, the certificate 58 includes a digital signature of a certification authority which generates the private key and the public key (hereinafter, a pair of these keys is called encryption keys) to assure the legitimacy of the certificate 58.

When the encryption module 23 receives the IC-card authentication request command and the common key, the CPU 10 of the user terminal 4 activates the IC-card driver 21 to operate the IC-card reading and writing unit 9 (in step SP5) to send the IC-card authentication request command C2 and the common-key-encrypted information to the IC card 8 through the IC-card reading and writing unit 9.

When the IC card 8 receives the IC-card authentication request command C2, the IC card 8 authenticates (decrypts) the common-key-encrypted information by the common key stored in the EEPROM 31 provided inside, and sends the result of authentication to the security server 6 through the encryption module 23 (in step SP5).

When the CPU 46 of the security server 6 confirms (in step SP15) from the received result of authentication that the IC card 8 has been successfully authenticated, the CPU 46 obtains the private key corresponding to the user ID (in step SP16) from the user-certificate data base 55 (Fig. 6) in response to the authentication request sent from the WWW server 3, generates a digital signature sheet (in step SP17) in which a digital signature has been applied to the received trial characters by the private key, and sends it (in step SP18) to the encryption module 23 of the user terminal 4.

Conversely, when the CPU 46 confirms (in step SP15) from the received result of authentication that the IC card 8 has not been successfully authenticated, the CPU 46 again receives the user ID, generates new common-key-encrypted information by using the common key corresponding to the user ID, and sends it to

the IC card 8. The CPU 46 again receives the result of authentication from the IC card 8.

When the encryption module 23 receives the digital signature sheet from the security server 6 (in step SP7), the CPU 10 of the user terminal 4 sends it to the WWW browser 10 through PKCS#11-24 (in step SP8). Then, the CPU 10 sends the received digital signature sheet to the WWW server 3 as the acknowledgement of the authentication request (in step SP9).

When the WWW server 3 receives the digital signature sheet, the WWW server 3 decrypts the digital signature by using the public key written into the user certificate received in advance. When the decryption is successfully performed, it is determined that the legitimate user terminal 4 has requested the electronic priced information.

The WWW server 3 prepares for sending the electronic priced information to the user terminal 4. The WWW server 3 encrypts the electronic priced information by the public key, and sends the encrypted electronic priced information to the user terminal 4.

In the network system 1, as shown in Fig. 12, the user terminal 4 performs writing according to a writing procedure RT3 shown in Fig. 13 and the security server 6 decrypts the encrypted electronic priced information according to a writing procedure RT4 shown in Fig. 14, so that the user terminal 4 writes the electronic priced information into the IC card 8.

The WWW server 3 sends the encrypted electronic priced information to the WWW browser 22 of the user terminal 4.

When the WWW browser 22 receives the encrypted electronic priced information, the CPU 10 of the user terminal 4 starts the writing procedure RT3 (in step SP21), and sends the received encrypted electronic priced information and a decryption request command C3 to the encryption module 23 (in step SP22).

Then, the CPU 10 sends the user ID read from the IC card 8 through the IC-card reading and writing unit 9, to the security server 6 together with the encrypted electronic priced information and the decryption request command C3 received by the encryption module 23 (in step SP23).

When the CPU 46 of the security server 6 receives the decryption request command C3, the CPU 46 starts the writing procedure RT4 (in step SP41) to authenticate the IC card 8. The CPU 46 reads the common key corresponding to the received user ID from the common-key data base 56 (in step S42), and generates common-key-encrypted information by using the read common key. Then, the CPU 46 sends the common-key-encrypted information and an IC-card authentication request command C4 to the encryption module 23 of the user terminal 4 (in step SP43).

When the encryption module 23 receives the IC-card authentication request command C4 and the common-key-encrypted information, the CPU 10 of the user terminal 4 operates the IC card driver 21 (in step SP24) to send the IC-card authentication request command C4 and the common-key-encrypted information to the IC card 8 through the IC-card reading and writing unit 9.

When the IC card 8 receives the IC-card authentication request command C4, it authenticates (decrypts) the common-key-encrypted information by using a common key stored in the EEPROM 31 provided therein, and sends the result of authentication to the security server 6 through the encryption module 23 (in step SP25).

The CPU 46 of the security server 6 receives the result of authentication sent from the encryption module 23 (in step SP44). When the CPU 46 confirms (in step SP45) from the result of authentication that the IC card 8 has been successfully authenticated, it obtains the private key corresponding to the user ID from the user-certificate data base 55 (Fig. 6) (in step SP46), and decrypts the encrypted electronic priced information by using the private key (in step SP47) to generate the electronic priced information.

Then, the CPU 46 encrypts the generated electronic priced information by using a common key read from the common-key data base 56 to generate common-key-encrypted electronic priced information.

When the CPU 46 confirms (in step SP45) from the received result of authentication that the IC card 8 has not been successfully authenticated, it receives the user ID from the user terminal 4, applies authentication to the common key

corresponding to the user ID within the IC card 8, and receives the result of authentication.

When the encryption module 23 receives a writing request command C5 and the common-key-encrypted electronic priced information from the security server 6 (in step SP27), the CPU 10 of the user terminal 4 sends the common-key-encrypted electronic priced information to the IC card 8 through the IC-card reading and writing unit 9.

The CPU 27 of the IC card 8 decrypts the received common-key-encrypted electronic priced information by using a common key read from the common-key area 34 of the EEPROM 31, and writes the electronic priced information obtained by decryption into the electronic-priced-information area 33 of the EEPROM 31.

The CPU 10 of the user terminal 4 sends the electronic priced information received by the encryption module 23 to the WWW browser 22. In this way, the WWW browser 22 obtains decrypted electronic priced information from the WWW server 3.

(3) Operations and advantages in the present embodiment

With the foregoing structure, in the network system 1, the security server 6 authenticates the user by the common-key encryption method by using the common key maintained in the IC card 8 which the user carries, in response to a user authentication request sent from the WWW server 3, and performs, only when the user has been authenticated, predetermined processing for making the WWW server 3 authenticate the user by the public-key encryption method.

Therefore, according to the network system 1, since the security server 6 authenticates the user by the common-key encryption method in response to a user authentication request sent from the WWW server 3, and performs, only when the user has been authenticated, predetermined processing for making the WWW server 3 authenticate the user by the public-key encryption method, quickness given by the common-key encryption method and safety given by the public-key encryption method are together provided.

According to the foregoing structure, in the network system 1, since the security server 6 authenticates the user by the common-key encryption method in response to a user authentication request sent from the WWW server 3, and

performs, only when the user has been authenticated, predetermined processing for making the WWW server 3 authenticate the user by the public-key encryption method, quickness given by the common-key encryption method and safety given by the public-key encryption method are together provided. Thus, the network system 1 has improved quickness and safety for authentication.

The user terminal is not limited to a personal computer. It may be a mobile communication apparatus, such as a portable telephone, a satellite telephone, a personal handyphone system (PHS), and a portable information terminal unit. The data holding apparatus is not limited to an IC card. It needs to hold a common key used in the common-key encryption method, but it does not necessarily have a card shape. It is preferred that the data holding apparatus be portable. The data holding apparatus and the user terminal may be integrated. The data holding apparatus may be a mobile communication apparatus in which an IC chip for an IC card is built in. In this case, the mobile communication apparatus may have a browser function for accessing information on the Internet and a reader/writer function for reading and writing an IC card.

(4) Other embodiments

In the foregoing embodiment, a case has been described in which the IC-card reading and writing unit 9 and IC card 8 send and receive information to and from each other by radio. The present invention is not limited to this case. The IC-card reading and writing unit 9 and the IC card 8 may be physically connected to send and receive information to and from each other.

In the foregoing embodiment, a case has been described in which authentication is first performed between the security server 6 and the IC card 8, and when electronic priced information decrypted by the security server 6 is stored in the IC card 8, authentication is again performed between the security server 6 and the IC card 8 and then the electronic priced information is stored in the IC card 8. The present invention is not limited to this case. Until a connection made between the security server 6 and the IC card 8 is broken, authentication may be performed only once between the security server 6 and the IC card 8.

In the foregoing embodiment, a case has been described in which, when the user terminal 4 sends a request for authentication to be performed with a common

key to the security server 6, the IC card 8 is authenticated. The present invention is not limited to this case. The IC card 8 may be authenticated in advance when the user terminal 4 is connected to the Internet and then to the security server 6.

In the foregoing embodiment, a case has been described in which electronic priced information such as electronic money and commuter-pass information is handled. The present invention is not limited to this case. Free information such as free software may be handled.

In the foregoing embodiment, a case has been described in which electronic money and commuter-pass information are handled as electronic priced information. The present invention is not limited to this case. Music information and book information may be handled as electronic priced information.

In the foregoing embodiment, a case has been described in which an IC card is used as an information holding medium. The present invention is not limited to this case. A medium having a calculation function and a memory function can be used.

In the foregoing embodiment, a case has been described in which encrypted information generated by the security server 6 by using a common key is decrypted by the IC card 8 to authenticate the user. The present invention is not limited to this case. Encrypted information generated by the IC card 8 by using a common key may be decrypted by the security server 6 to authenticate the user.

Although the present invention has been described with reference to specific embodiments, those of skill in the art will recognize that changes may be made thereto without departing from the spirit and scope of the invention as set forth in the hereafter appended claims.